

Polityka Certyfikacji dla Certyfikatów PEMI

wersja 1.0

Spis treści:

1	Wprowadzenie.....	3
1.1	Identyfikator polityki	3
1.2	Historia zmian.....	3
1.3	Dane kontaktowe	3
2	Postanowienia polityki	3
2.1	Odbiorcy usług certyfikacyjnych (subskrybent)	3
2.2	Prawa i obowiązki stron.....	4
2.2.1	Obowiązki posiadaczy certyfikatów (subskrybentów)	4
2.2.2	Obowiązki stron ufających.....	4
2.3	Odpowiedzialność Centrum Certyfikacji.....	4
2.4	Publikowanie i Repozytorium.....	4
2.5	Poufność	4
3	Złożenie wniosku o certyfikat (Rejestracja)	5
3.1	Certyfikaty do podpisu, szyfrowania, uwierzytelniania	5
3.2	Certyfikaty VPN/SSL	5
3.3	Certyfikaty WWW	5
3.4	Certyfikaty podpisywanie kodu	6
4	Unieważnianie certyfikatów	6
5	Odnawianie certyfikatów	6
6	Profil listy certyfikatów Unieważnionych (CRL).....	7

Podstawowe definicje:

subskrybent – osoba fizyczna, firma lub instytucja która uzyskała certyfikat i się nim posługuje (jest jego właścicielem- posiada klucz prywatny powiązany z certyfikatem) np. podpisuje elektronicznie dane

strona ufająca – osoba fizyczna, firma lub instytucja która korzysta z certyfikatów w celu zweryfikowania poprawności użycia klucza prywatnego np. weryfikuje podpis złożony przez subskrybenta przy pomocy klucza prywatnego.

polityka certyfikacji - niniejszy dokument

1 Wprowadzenie

1.1 Identyfikator polityki

Nazwa polityki	Polityka Certyfikacji dla certyfikatów PEMI
Wersja	1.0
Status wersji	aktualny

1.2 Historia zmian

Wersja	Data	Opis zmian
1.0	20.10.2004	Powstanie dokumentu

1.3 Dane kontaktowe

Więcej informacji można uzyskać pod adresem :
Stowarzyszenie PEMI „Podpis elektroniczny – Mobile - Internet”
Centrum Certyfikacji PEMI
ul Stefana Bryły 3 /582
02-685 Warszawa
KRS 0000213935
Mail: polityka@podpiselektroniczny.pl

2 Postanowienia polityki

2.1 Odbiorcy usług certyfikacyjnych (subskrybent)

Posiadaczem certyfikatu jest osoba fizyczna, firma lub instytucja, która złożyła wniosek o certyfikat

W ramach **Polityki** wydawane są dwuletnie certyfikaty przeznaczone odpowiednio do podpisywania/weryfikacji , szyfrowania/desyfrowania , uwierzytelniania lub dla urzędzeń

Certyfikaty wydawane zgodnie z niniejszą **Polityką** nie mogą być wykorzystywane w żadnym innym celu niż określony powyżej.

2.2 Prawa i obowiązki stron

2.2.1 Obowiązki posiadaczy certyfikatów (subskrybentów)

Posiadacz certyfikatu (subskrybent) zobowiązany jest do ochrony własnego klucza prywatnego oraz hasła do zarządzania certyfikatem.

Osoba wnioskująca o certyfikat zobowiązana jest zadbać o prawidłowość, dokładność, prawdziwość danych podawanych we wniosku o wydanie certyfikatu.

Posiadacz certyfikatu w przypadku zmiany danych lub kompromitacji klucza zobowiązany jest unieważnić swój certyfikat

Za dane zawarte w certyfikacie odpowiada osoba wnioskująca o certyfikat

2.2.2 Obowiązki stron ufających

Strona ufająca przed podjęciem decyzji o zaufaniu do danego certyfikatu weryfikuje czy sposób przeprowadzenia weryfikacji danych był dla niej wystarczający. Informacje na temat weryfikacji danych umieszczone są w punkcie 3 „Rejestracja”. Centrum Certyfikacji PEMI nie ponosi odpowiedzialności za szkody wynikłe z niewłaściwego użytkowania certyfikatu. Jeśli strona ufająca nie posiada odpowiedniego poziomu wiedzy do podjęcia decyzji o zaufaniu powinna skontaktować się z weryfikacja@podpiselektroniczny.pl

2.3 Odpowiedzialność Centrum Certyfikacji

Centrum Certyfikacji PEMI jest odpowiedzialne za umieszczanie w certyfikacie danych przekazanych przez wnioskodawcę. Centrum Certyfikacji PEMI nie ponosi odpowiedzialności za szkody wynikłe w związku z niewłaściwym użyciem certyfikatów wydanych przez Centrum Certyfikacji PEMI.

2.4 Publikowanie i Repozytorium

Certyfikaty oraz listy certyfikatów unieważnionych wydane zgodnie z niniejszą polityką publikowane są w ogólnie dostępnym repozytorium pod adresem www.podpiselektroniczny.pl/repozytorium/

Lista certyfikatów unieważnionych dla certyfikatów wydawanych zgodnie z niniejszą polityką tworzona jest co godzinę.

2.5 Poufność

Centrum Certyfikacji PEMI udostępnia jedynie informacje zawarte w certyfikatach.

3 Złożenie wniosku o certyfikat (Rejestracja)

Proces rejestracji (złożenia wniosku) polega na przesłaniu do Centrum certyfikacji wniosku o certyfikat. Wniosek przygotowywany jest wcześniej lub generowany bezpośrednio na stronie rejestracji. Złożony wniosek wymaga zaakceptowania przez administratora PEMI. W niektórych przypadkach weryfikowany jest również dostęp wnioskodawcy do konta poczty elektronicznej podanego w procesie rejestracji.

3.1 Certyfikaty do podpisu, szyfrowania, uwierzytelniania

Etapy uzyskania certyfikatu (weryfikowany jest jedynie dostęp użytkownika do danego adresu poczty elektronicznej):

- Użytkownik (subskrybent) wyraża zgodę na przetwarzanie danych oraz akceptuje zapisy odpowiedniej polityki certyfikacji
- Następnie wypełnia formularz na stronie WWW, w formularzu podaje dane do certyfikatu, adres poczty elektronicznej oraz hasło do zarządzania certyfikatem
- Następnie generuje parę kluczy kryptograficznych (publiczny i prywatny). Do centrum certyfikacji zostaje wysłany wniosek o certyfikat oraz klucz publiczny
- Na adres poczty elektronicznej podany we wniosku zostaje wysłana wiadomość z odnośnikiem do wystawionego certyfikatu (w ten sposób zostaje zweryfikowany dostęp użytkownika do danego adresu poczty elektronicznej)
- Użytkownik znając ten odnośnik może zainstalować właściwy certyfikat

UWAGA !!! wysłanie wiadomości na adres poczty elektronicznej nie daje 100% gwarancji że użytkownik posiadał dostęp do tego konta

3.2 Certyfikaty VPN/SSL

Etapy uzyskania certyfikatu:

- Użytkownik (subskrybent) wyraża zgodę na przetwarzanie danych oraz akceptuje zapisy odpowiedniej polityki certyfikacji
- Następnie w specjalnym formularzu wkleja wygenerowane wcześniej żądanie certyfikatu (Request). Uzupełnia o adres poczty elektronicznej oraz hasło do zarządzania certyfikatem
- Na adres poczty elektronicznej podany we wniosku zostaje wysłany wygenerowany certyfikat
- Użytkownik może zainstalować otrzymany certyfikat

UWAGA !!! wysłanie wiadomości na adres poczty elektronicznej nie daje 100% gwarancji że użytkownik posiadał dostęp do tego konta

3.3 Certyfikaty WWW

Etapy uzyskania certyfikatu:

- Użytkownik (subskrybent) wyraża zgodę na przetwarzanie danych oraz akceptuje zapisy odpowiedniej polityki certyfikacji
- Następnie w specjalnym formularzu wkleja wygenerowane wcześniej żądanie certyfikatu (Request). Uzupełnia o adres poczty elektronicznej oraz hasło do zarządzania certyfikatem
- W celu zweryfikowania dostępu do danego serwera użytkownik umieszcza w katalogu głównym serwera wygenerowane wcześniej żądanie (Request)
- Jeśli administrator potwierdzi obecność właściwego żądania na serwerze na adres poczty elektronicznej podany we wniosku zostaje wysłany certyfikat
- Użytkownik może zainstalować otrzymany certyfikat

UWAGA !!! wysłanie wiadomości na adres poczty elektronicznej nie daje 100% gwarancji że użytkownik posiadał dostęp do tego konta

3.4 Certyfikaty podpisywanie kodu

Etapy uzyskania certyfikatu:

- Użytkownik (subskrybent) wyraża zgodę na przetwarzanie danych oraz akceptuje zapisy odpowiedniej polityki certyfikacji
- Następnie w specjalnym formularzu wkleja wygenerowane wcześniej żądanie certyfikatu (Request). Uzupelnia o adres poczty elektronicznej oraz hasło do zarządzania certyfikatem
- Na adres poczty elektronicznej podany we wniosku zostaje wysłany wygenerowany certyfikat
- Użytkownik może zainstalować otrzymany certyfikat

UWAGA !!! wysłanie wiadomości na adres poczty elektronicznej nie daje 100% gwarancji że użytkownik posiadał dostęp do tego konta

4 Unieważnianie certyfikatów

Unieważnianie certyfikatu realizowane jest poprzez dedykowany interfejs (następuje po pozytywnej weryfikacji wprowadzonego hasła do zarządzania certyfikatem).

5 Odnawianie certyfikatów

Odnowienie certyfikatu odbywa się na nowo wygenerowanej parze kluczy

6 Profil listy certyfikatów Unieważnionych (CRL)

Lista certyfikatów unieważnionych wskazana w certyfikacie wystawionym zgodnie z niniejszą **Polityką** zawiera:

Atrybut	Wartość
version	1 # lista zgodna z wersją 2 standardu X.509
signature	SHA1WithRSAEncryption # nazwa algorytmu stosowanego do podpisywania listy CRL
issuer	# nazwa wyróżniona jednostki wystawiającej certyfikaty zgodne z niniejszą Polityką
country (C)	PL
state/province (ST)	
locality (L)	
organisation (O)	
organizationalUnit (OU)	
commonName (CN)	
thisUpdate	# data i godzina wydania listy
nextUpdate	# data i godzina następnego wydania listy
revokedCertificates	# lista odwołanych certyfikatów
userCertificate	# numer seryjny unieważnionego certyfikatu
revocationDate	# data i godzina
reasonCode	# przyczyna umieszczenia certyfikatu na liście CRL

Do przyczyn umieszczenia certyfikatu na liście zalicza się:

unspecified (0)	nieokreślona
keyCompromise (1)	kompromitacja klucza
cACompromise (2)	kompromitacja klucza CC
affiliationChanged (3)	zmiana danych posiadacza certyfikatu
superseded (4)	zastąpienie (odnowienie) klucza
cessationOfOperation	zaprzestanie używania certyfikatu do celu, w jakim został wydany
certificateHold (6)	certyfikat został zawieszony